IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
	)	
William J. Yarborough	)	Confirmation No. 3635
	)	
Serial No.: 10/006,484	)	Art Unit: 2135
	)	
Filed: December 5, 2001	)	Examiner: PAN, Joseph T.
	)	
Docket No.: 72167.000295	)	

For: SECURED FTP ARCHITECTURE

Mail Stop ***Appeal Brief - Patents***
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

TABLE OF CONTENTS

Page

I. Real Party In Interest 4
II. Related Appeals and Interferences 4
III. Status of Claims 4
IV. Status of Amendments 4
V. Summary of Claimed Subject Matter 5
VI. Grounds of Rejection to be Reviewed on Appeal 6
VII. Argument 7
A. Summary of Argument 7
B. Independent Claim 1 is Patentable over the Cited References 7
1. The Sit-Underwood Combination Fails to Teach or Suggest All the Elements in the Claimed Invention 9
2. There Is No Suggestion or Motivation to Combine or Modify Sit and Underwood. 14
3. The Examiner Fails to Consider the Claimed Invention "As a Whole." 17
C. Independent Claim 12 is Patentable over the Cited References 21
D. Dependent Claims 2-11 and 13-25 Are Each Separately Patentable Over the Cited References 21
VIII. Claims Appendix 22
IX. Evidence Appendix 22
X. Related Proceedings Appendix 22
XI. Conclusion 23
Appendix A: Listing of Claims 24

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
	)	
William J. Yarborough	)	Confirmation No. 3635
	)	
Serial No.: 10/006,484	)	Art Unit: 2135
	)	
Filed: December 5, 2001	)	Examiner: PAN, Joseph T.
	)	
Docket No.: 72167.000295	)	

For: SECURED FTP ARCHITECTURE

Mail Stop ***Appeal Brief - Patents***
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant's Appeal Brief in connection with the above-captioned patent application (hereinafter "the present application") is hereby submitted in triplicate. The requisite fee in accordance with 37 C.F.R. §41.20(b)(2) is enclosed. It is respectfully submitted that this Appeal Brief is timely filed in support of the Notice of Appeal filed on October 30, 2006. Each item required by 37 C.F.R. §41.37 is set forth below. Appellant believe that no additional fees are necessary. However, if there are any deficiencies, please charge the undersigned's Deposit Account No. 50-0206.

In response to the Final Office Action dated June 29, 2006, rejecting pending claims 1-25, Appellant respectfully request that the Board of Patent Appeals and Interferences reconsider and withdraw the rejection of record, and allow the pending claims, which are attached hereto as Appendix A.

I. REAL PARTY IN INTEREST

The Appellant, William Jordan Yarborough, is the sole inventor and Applicant in the above-identified patent application. The Appellant has assigned his entire interest in the above-identified patent application to JPMorgan Chase Bank, having a place of business at 270 Park Ave., New York, NY 10017.

II. RELATED APPEALS AND INTERFERENCES

The Appellant, the Appellant's legal representative, and the Assignee are not aware of any other appeals or interferences which will directly affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. STATUS OF CLAIMS

Claims 1-25 are pending in the above-identified patent application. Claims 1-25 were finally rejected in an Office Action dated June 29, 2006. The final rejection of claims 1-25 is hereby appealed.

Claims 1-2, 11-13 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sit *et al.* (U.S. Patent 6,349,336, hereinafter "Sit") in view of Underwood (U.S. Patent 6,718,535, hereinafter "Underwood"). Claims 3-4 and 14-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sit, in view of Underwood, and further in view of Fan *et al.* (U.S. Patent 6,219,706, hereinafter "Fan"). Claims 5-10 and 16-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sit in view of Underwood and Fan, and further in view of Albert *et al.* (U.S. Patent 6,687,222, hereinafter "Albert").

IV. STATUS OF AMENDMENTS

The above-identified patent application was filed on December 5, 2001, claiming priority to U.S. Provisional Application No. 60/325,634 filed on September 28, 2001. A first Office

Action was issued on May 27, 2005, rejecting claims 1-25. On August 29, 2005, a Response was filed in response to the first Office Action, in which no amendment was made. A Final Office Action was issued on November 4, 2005, maintaining rejection of claims 1-25. On January 11, 2006, a Request for Continued Examination was filed in response to the Final Office Action. Another Non-final Office Action was issued on February 24, 2006, rejecting claims 1-25 on slightly different grounds. On April 7, 2006, a Response was filed in response to the Non-final Office Action, in which no amendment was made. Another Final Office Action was issued June 29, 2006, maintaining the rejection of claims 1-25. On October 30, 2006, a Notice of Appeal was filed.

No substantive amendment has been made in the claims. Appellant hereby appeals the final rejection of the originally filed claims 1-25.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention, as set forth in claim 1, and as described in the specification of the above-identified patent application, is directed to a system for providing secure transfer of data. The system may comprise: a client system (e.g., Figure 2: FTP client system **2**); a server (e.g., Figure 2: FTP server **4**); a security system (e.g., Figure 2: center box between PUBLIC NETWORK **6** and PRIVATE NETWORK **8**) interposed between said client system (**2**) and said server (**4**) for controlling communications between said client system and said server. The security system may include: a first proxy system (e.g., Figure 2: FTP client proxy system **12**) and a second proxy system (e.g., Figure 2: FTP server agent **14**), said first proxy system (**12**) coupled between said client system (**2**) and said second proxy system (**14**), and said second proxy system (**14**) coupled between said server (**4**) and said first proxy system (**12**). The security system may further include a firewall (e.g., Figure 2: firewall **10**) coupled between said first

proxy system (**12**) and said second proxy system (**14**), said firewall (**10**) restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall. All FTP data are transferred between said client system (**2**) and said server (**4**) through said single port on said firewall (**10**). *See* present application, paragraph [0030]-[0046] and Figures 2-4.

The present invention, as set forth in claim 12, and as described in the specification of the above-identified patent application, is also directed to a method for providing secure transfer of data. The method may comprise: using a client system (**2**) to request data (**S100**, **S102**, **S114**, **S126**); using a server (**4**) to provide data (**S110**, **S118**, **S130**); controlling communications between said client system and said server using a security system (**S104-S108**, **S116**, **S120-S124**, **S128**, **S132**, **S134**). The security system may include: a first proxy system (**12**) and a second proxy system (**14**), said first proxy system coupled between said client system and said second proxy system, and said second proxy system coupled between said server and said first proxy system. The security system may also include a firewall (**10**) coupled between said first proxy system and said second proxy system, said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall. The method may further comprise: using said security system to transfer said data between said client and said server (**S116-S122**, **S132**, **S134**); and restricting all flow of FTP data passing through said security system through a single port on said firewall (Figures 3 and 4). *See* present application, paragraph [0047]-[0051] and Figure 5.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection is that claims 1-25 are obvious under 35 U.S.C. §103(a) in view of the cited references Sit, Underwood, Fan and Albert. Allegedly, claims 1-2, 11-13 and 25 are

unpatentable over Sit in view of Underwood; claims 3-4 and 14-15 are unpatentable over Sit, in view of Underwood, and further in view of Fan; claims 5-10 and 16-24 are unpatentable over Sit in view of Underwood and Fan, and further in view of Albert.

VII. ARGUMENT

A. Summary of Argument

Appellant respectfully submits that the rejection of claims 1-25 under 35 U.S.C. §103(a) is improper. Under 35 U.S.C. §103, the Patent Office bears the burden of establishing a *prima facie* case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The Patent Office can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of references. Id. Further, as stated in M.P.E.P. §2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Appellant respectfully submits that the Examiner has not met the burden of proof in establishing the obviousness of the appealed claims 1-25.

B. Independent Claim 1 is Patentable over the Cited References

The obviousness rejection of claim 1 is improper for at least the following reasons: (1) the combination of Sit with Underwood fails to teach or suggest all the elements recited in claim 1; (2) there is no suggestion or motivation in the cited references or in the general knowledge to make the combination; and (3) the Examiner failed to consider the claimed invention "as a whole."

Before discussing this ground of rejection, a brief summary of a preferred embodiment of Applicant's invention is provided in order to highlight some of its advantageous characteristics. A brief summary of Sit and Underwood is also provided for comparison.

The present invention, as recited in independent claim 1, is directed to a secured file transfer protocol (FTP) system. Embodiments of the present invention specifically address the difficulties faced by a FTP client behind a firewall. In one embodiment, two FTP proxy systems (e.g., a FTP client proxy system **12** and a FTP server agent **14** in Figure 2) are positioned astride a firewall device (e.g., a firewall **10** in Figure 2). The client-side FTP proxy system (e.g., the FTP client proxy system **12**) has a FTP-like session with the FTP client. The server-side FTP proxy system (e.g., the FTP server agent **14**) has a FTP-like session with the FTP server. The two FTP proxy systems may communicate with each other securely across the firewall device via a single port on the firewall. One advantage of such an embodiment is to prevent the firewall from opening and closing random ports as in traditional FTP sessions. As a result,

> "the passive FTP client systems **2** are protected from attacks by users in the public network because firewall **10** does not allow session request connections originating from the public network side. The FTP control connection is initiated from the private network side of the firewall **10** by the FTP client proxy system **12**, connecting outward to the FTP server agent **14**. Thus, even if a hacker were able to compromise FTP server agent **14**, the hacker would not be unable to jump from FTP server agent **14** to the FTP client proxy system **12** because internal fire wall **10** is configured to deny inbound requests.
>
> "Furthermore, the present invention advantageously employs the use of software modules executing on the passive FTP client system 2, proxy client system 12 and FTP server agent 14 which provides seamless integration with the firewalls and proxy servers that are provided by service providers. In particular, these software modules function to allow multiple passive FTP client systems 2 to access destination FTP servers 4 using a single or minimal number of TCP/IP addresses and logical communication ports while simultaneously providing application level security and encryption services."

present application: paragraphs [0052]-[0053].

Sit discloses a hypertext transfer protocol (HTTP) tunneling action that allows a remote processor to communicate with a local processor when the remote processor is coupled to the

local processor via a reverse proxy device, a computer network, a firewall and a proxy agent device. The primary goal in Sit is to trick the firewall into believing that an incoming request is actually a response to an outgoing request, so that the remote processor may access/control the local processor behind the firewall. *See* Sit: col. 2, lines 39-60 and col. 3, lines 36-48.

Underwood is directed to a system and method for providing an activity framework in an e-commerce based environment. Underwood includes a voluminous survey of software framework designs. However, it is believed that the Examiner now relies on Underwood only for its disclosure of using proxy services for FTP. *See* Underwood: col. 104, line 65 - col. 105, line 2.

1. The Sit-Underwood Combination Fails to Teach or Suggest All the Elements in the Claimed Invention.

As stated in M.P.E.P. §2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (C.C.P.A. 1974).

Individually or in combination, Sit and Underwood do not disclose or even suggest (i) "*said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall*" or (ii) "*wherein all FTP data are transferred between said client system and said server through said single port on said firewall*" as recited in claim 1. Therefore, the Sit-Underwood combination cannot render the claimed invention obvious.

It is unclear, based on the June 29, 2006 Final Office Action (hereinafter "Final Office Action"), as to where in the prior art the Examiner finds the use of a single firewall port (for FTP services).

On the one hand, the Examiner conceded that "Sit et al. do not specifically mention using a single port on the firewall," and "Sit et al. also do not specifically mention that the system supports FTP." Final Office Action at page 3. Indeed, a search in its disclosure reveals that Sit never even uses the terms "port," "FTP" or "file transfer protocol." The Examiner then went on to assert that "it's well-known in the art of the computer network that using a single port on the firewall, instead of opening multiple ports, increases the security of the network" (Final Office Action at page 4). Therefore, it appeared that the Examiner was taking an official notice of the claimed feature of using a single port on a firewall.

On the other hand, however, the Examiner alleged that "Examiner's primary reference Sit et al. already disclose using the single port feature on the firewall, Examiner mainly uses Underwood reference for the FTP feature" (Final Office Action at page 13). Here, the Examiner appeared to be referring to his reasoning on page 11 of the Final Office Action, where it was asserted that, since "it's well known in the art that HTTP communications use single port 80" (and because Sit discloses HTTP communications), "Sit et al. disclose (i) restricting HTTP data flow ... to outbound communications through a single port on said firewall ... or (ii) restricting all flow of HTTP data passing through said security system through a single port on said firewall" (emphasis in original). Thus, the Examiner appeared to believe that Sit did disclose the use of a single firewall port after all.

Wherever the Examiner purports to find a prior art disclosure of using a single port on a firewall, the Examiner's ground of rejection would be flawed.

To the extent that the Examiner finds the use of a single firewall port to be "well known" in the art, there is no support in the record for the conclusion that the identified feature is "old and well known." In accordance with M.P.E.P. §2144.03, the Examiner must cite a reference in

support of his position. As will be explained below, even if the use of a single firewall port were old and well known, the mechanical assembly of the discrete elements found in the cited references still cannot support the obviousness rejection of claim 1.

To the extent that the Examiner finds the use of a single port on a firewall to be implied disclosed in Sit (i.e., by virtue of its disclosure of HTTP), the Examiner's subsequent reasoning fails to bridge a logical gap from "single-port HTTP" to "single-port FTP."

HTTP and FTP protocols are fundamentally different in terms of their connection procedures and the number of ports required.

HTTP/1.1 standard mandates a "persistent connection" between an HTTP client and an HTTP server. Fielding, et al., Hypertext Transfer Protocol -- HTTP/1.1,[1] Network Working Group RFC-2616, June 1999, page 43 ("HTTP implementations SHOULD implement persistent connections."). "HTTP communication usually takes place over TCP/IP connections. The default port is TCP 80." Id. at page 12. Thus, for an HTTP session, whether or not it is through a firewall, a single persistent connection between an HTTP client and a web server is the norm.

For an FTP session, multiple connections, rather than a single persistent connection, between an FTP client and an FTP server is required. According to the prevailing FTP standard, a typical FTP session needs at least two TCP connections, one control connection and one data connection. Postel et al, File Transfer Protocol (FTP), Network Working Group STD-9 (RFC-959), October 1985, pages 4 and 8. In contrast to the "persistent connection" requirement in HTTP/1.1, the FTP standard specifically notes that "the data connection need not exist all of the time" (Id. at page 8). In the present application, the control connection is referred to as a "command channel," and the data connection is referred to a "data channel."

[1] All the articles cited in this Appeal Brief have been submitted with prior filings and should be on record.

It should be noted, however, that the standard two-connection FTP model is not strictly followed by real-world FTP operations. Although "[t]he FTP specification says that by default, all data transfers should be over a single connection, ... most current FTP clients do not behave that way." Bellovin, Firewall-Friendly FTP, Network Working Group RFC-1579, February 1994, page 1. Instead, "[a] new connection is used for each transfer; to avoid running afoul of TCP's TIMEWAIT state, the client picks a new port number each time and sends a PORT command announcing that to the server." Id. Alternatively, "if the client sends a PASV command, the server will do a passive TCP open on some random port, and inform the client of the port number. The client can then do an active open to establish the connection." Id. Therefore, in reality, more than two TCP connections are typically used for each FTP session and some connections involve random ports, making FTP sessions even more complicated than HTTP sessions.

When a firewall is involved, the implementation of FTP protocol would be even more different from (and more complicated than) HTTP protocol. Because of the multiple-connection requirement, an FTP session through a firewall often requires the opening and closing of multiple random ports in the firewall to accommodate the data connections. That is, a firewall port randomly assigned for one FTP data connection does not remain open indefinitely. *See* present application: Figure 1 and paragraph [0016] ("After requested data are sent to the passive FTP client system 2 by the FTP server 4 over the data channel, the FTP server 4 and the firewall 10 dynamically close the corresponding logical communication ports until the next data channel transmission.").

In view of the foregoing comparison of HTTP and FTP, it may be appreciated that the use of a single firewall port for HTTP purposes would not prompt one of ordinary skill in the art

to contemplate the use of a single firewall port for FTP purposes. Contrary to the false impression that the Examiner would like to make, it is not such an obvious or trivial step to go from "single-port HTTP" to "single-port FTP."

In order to solve the problems uniquely associated with FTP sessions through a firewall, an artisan must first identify such problems. As recognized in the present application, the specific problems include, for example, the "potential security exposures" caused by "dynamic opening and closing of ports on a firewall," and the "significant administrative resources" "required to configure a firewall to allow communication over a large range of sources and destinations" (present application: paragraph [0018]). The recognition of such problems is an essential part of the present invention, which leads to a secured FTP architecture as recited in claim 1. Yet, there is no indication in any of the cited references that these problems were ever recognized or identified prior to the time of the present invention. Nor are these problems easily recognizable by a person of ordinary skill in view of the two-connection FTP model specified in the prevailing standard.

Further, Sit and Underwood do not say anything about restricting all (HTTP) data flow to a single port in the firewall. While one connection is kept open between the two proxy devices for one HTTP session, there is no suggestion that the same connection will be used for all HTTP sessions (i.e., all data flows) between the two proxy devices. As such, multiple random ports (or TCP sockets) may still be opened and closed in the firewall for multiple HTTP sessions. Note that port 80 is merely a default port for HTTP; but HTTP/1.1 does not require a web server or firewall to use the same port for all HTTP sessions. In the present invention, however, "a single outbound connection between the FTP client proxy system 12 and the FTP server agent 14 uses a single port on the firewall 10 and multiplexes a plurality of FTP sessions between a plurality of

FTP servers 4 and a plurality of passive FTP client systems 2" (present application: paragraph [0046,]emphasis added). *See also*, Figures 3 and 4.

Furthermore, claim 1 requires "*said firewall restricting [all] data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall.*" Sit and Underwood do not teach or suggest this feature. In Sit and for HTTP across a firewall in general, it is the (web) server that is behind the firewall. In the present application, however, it is the (FTP) client that is behind the firewall. Underwood mentions that an HTTP proxy can control outbound traffic, but "these controls generally do not apply to inbound traffic" (Underwood: col. 281, lines 49-55). Therefore, neither Sit nor Underwood discloses a restriction of all data flow to "outbound communications through a single port on said firewall" as recited in claim 1.

Since neither Sit nor Underwood teaches or suggests (i) "*said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall*" or (ii) "*wherein all FTP data are transferred between said client system and said server through said single port on said firewall,*" the Sit-Underwood combination cannot render the claimed invention obvious.

2. There Is No Suggestion or Motivation to Combine or Modify Sit and Underwood.

As stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Since no such "teaching, suggestion, or motivation" can be found in the cited references or in general knowledge, the obviousness rejection of claim 1 is improper.

The text of Sit does not provide any explicit suggestion or motivation to combine with Underwood. Sit makes no reference whatsoever to the terms "FTP" or "file transfer protocol." Therefore, as the Examiner concedes in page 3 of the Office Action, Sit provides no explicit motivation to modify its system for FTP sessions.

Neither is there any implicit suggestion for the modification. First, Sit focuses exclusively on HTTP sessions, which are completely different from typical FTP sessions in terms of the required number of connections and firewall ports. It is hardly obvious how such a HTTP-specific implementation could prompt someone to adapt it for the kind of FTP traffic as described in the present application. Second, Sit's primary goal is to allow an outside computer to access and control a local computer behind a firewall. To achieve this goal, Sit implements two HTTP proxies to trick the firewall into believing the incoming requests are responses to some outgoing requests. *See* Sit: col. 7, line 50 - col. 8, line 12. This trickery on the firewall achieves exactly what a secured FTP architecture tries to avoid. In the present invention, the security of the firewall is not in anyway circumvented or compromised. Claim 1 recites "said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall." Thus, the firewall in the present invention still functions as it is designed to. All FTP data between a local FTP client and an external FTP server are multiplexed onto a single-port secured connection between the two proxy systems. It is difficult to imagine that a network engineer who is mindful of firewall security would be inspired by Sit's security-bypass measures to build a secured FTP system as claimed.

Nor does Underwood provide any suggestion or motivation to combine with Sit.

First, Underwood is focused on e-Commerce which is known to be dominated by the use of Web browsers with HTML language. According to Underwood, "[a] preferred embodiment of the invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol for a transport medium between the client and a company." Underwood: col. 15, line 64 - col. 16, line 1. A cursory review of Underwood would reveal that its disclosure is mostly concerned with HTTP.

Second, Underwood does not even use FTP protocol for file transfer services. Underwood's system is referred to as "Resources eCommerce Technology Architecture (ReTA)." Underwood: col. 10, lines 22-23. "ReTA implements file transfer services through Microsoft's Internet Information Server 4.0 (IIS) using the HyperText Transfer Protocol (HTTP)." Underwood: col. 115, lines 37-39. Underwood apparently favors HTTP over FTP because "HTTP reduces the inefficiencies of the FTP protocol." Underwood: col. 115, line 43.

In addition, Underwood suggests "Do not mix HTTP with anonymous FTP." Underwood: col. 302, line 33.

In view of Underwood's preference for HTTP, its rejection of FTP, and its advice of not mixing these two protocols, it is inconceivable that Underwood could ever provide any suggestion or motivation to combine with Sit's HTTP-oriented system in order to build a secure FTP system as recited in claim 1.

Since neither Sit nor Underwood provides any motivation to combine, in order for the obviousness rejection to stand, such motivation must come from the knowledge generally available to one of ordinary skill in the art. However, that is not the case here either. As discussed above, in order to solve the problems uniquely associated with FTP sessions through a

firewall, an artisan must first identify such problems as the "potential security exposures" caused by "dynamic opening and closing of ports on a firewall." The recognition of such problems is an essential part of the present invention, which leads to a secured FTP architecture as claimed. Yet, there is no indication in the cited references that these problems were ever recognized or identified prior to the time of the present invention. Without recognizing the particular "FTP-through-firewall" problems, a person of ordinary skill in the art would not make a radical departure from the standard two-connection (thus two-port) FTP model that has been well accepted by the Internet community.

Further, the HTTP-based Sit system cannot be mechanically combined with Underwood for implementation of a secured FTP system as claimed. Even if Sit and Underwood were technologically combinable, their combination would be legally improper, for the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Since the record does not show the desirability of the Sit-Underwood combination in the prior art, the combination cannot render the claimed invention obvious.

Since the requisite suggestion or motivation is not found in the cited references or in common knowledge, the obviousness rejection of claim 1 cannot stand.

3. The Examiner Fails to Consider the Claimed Invention "As a Whole."

By focusing on the structural similarity between Sit and the claimed system while trivializing their technological differences, the Examiner has failed to consider the claimed invention "as a whole."

As stated in M.P.E.P. §2141.02, in determining the differences between the prior art and the claims, the question under 35 U.S.C. §103 is not whether the differences themselves would

have been obvious, but whether the claimed invention as a whole would have been obvious. "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (C.C.P.A. 1970).

The Examiner has issued four office actions rejecting the originally filed claims 1-25. The four office actions were substantially similar and were based on the same flawed strategy. Essentially, the Examiner has clung to the primary reference Sit because it discloses a physical arrangement of network components (Sit: Figure 5) that looks quite similar to an illustrated embodiment (Figure 2) of the present invention. Appellant does not deny the apparent structural similarity between Sit and the claimed system. However, even the Examiner concedes that Sit by itself is insufficient for the claim rejection. Nevertheless, the Examiner appeared to be overly content with this primary reference and so far has only made cursory attempts to mechanically patch up the deficiencies in Sit with various secondary references.

The evolving grounds of the obviousness rejection in the four office actions might be illuminating. The Examiner started off by citing Epstein *et al.* (U.S. Patent 6,584,508, hereinafter "Epstein") to remedy Sit's failure to disclose an FTP function. *See* May 27, 2005 Office Action. When Applicant pointed out Sit's limitation to HTTP context as well as its failure to disclose the use of a single firewall port for FTP services, the Examiner responded with a final rejection, essentially alleging that: (i) Sit's passing reference to Simple Mail Transfer Protocol (SMTP) made the adaptation of Sit's system for FTP obvious (*see* November 4, 2005 Office Action at pages 8-9); (ii) Figure 5 in Sit by itself suggested multiplexing capability (Id.); and (iii) the prior art structure was "capable of performing the intended use" and therefore met the claimed limitations (Id. at page 10).

Later, in the February 24, 2006 Office Action, the Examiner dropped those spurious allegations and replaced Epstein with the 279-page Underwood patent. The Examiner attempted to use Underwood to provide the "single-port FTP" feature that is missing in the primary reference Sit. However, the Examiner's reliance on Underwood turned out to be misplaced as well, because the Examiner confused the default port 1080 reserved on a SOCKS proxy with the single firewall port for FTP services. Apparently acknowledging this error, the Examiner gave up his allegation that Underwood disclosed a single firewall port for FTP and maintained that Underwood was cited only for its disclosure of an FTP feature. Final Office Action at page 13.

Therefore, after all these office actions, prosecution of the present application is essentially back to square one — Sit remains the primary reference while Underwood, despite its volume, is reduced to the same role as the initially cited Epstein. The Examiner's grounds of rejection have never been legally or technically sufficient to necessitate any amendment in the claims.

The Examiner's approach to the obviousness rejection may be summarized as a "picture-plus-keywords" strategy. The Examiner chose Sit as the primary reference due to its structural similarity as shown in Figure 5. Beyond that, the Examiner did nothing more than searching for the key terms "single port" and "FTP" in order to come up with the secondary references. The combination of Sit with the secondary references are made with no regard to the context of the primary and second references or whether they are technologically combinable.

The flaws in the claim rejections are obvious. Apparently, the Examiner was so content with the primary reference Sit that it became somewhat entrenched in his mind. As a result, the Examiner has been quite reluctant to step further beyond the mere structural similarity to locate

legally and technologically combinable references, and thereby has failed to give the claimed invention a fair evaluation against the prior art references.

The Examiner's over-reliance on the structural similarity is inappropriate for both the system and method claims currently on appeal. Appellant do not deny the substantial physical resemblance between the Sit system and what is disclosed in the present application. However, physical resemblance does not preclude the patenting of a new system if it is adapted from an old system to perform a new and novel function. In fact, even if the new system as recited in claim 1 were physically or structurally identical to the old system as depicted in Sit, the programming of the old system to perform an inventive function would still make the new system patentable over the old. *See* In re Alappat, 33 F.3d 1526, 1542-1545 (Fed. Cir. 1994)(en banc)(programming creates new machine, as general purpose computer became, in effect, special purpose computer once it was programmed to perform particular functions pursuant to instructions from program software). In the present application, the inventive function includes the use of a single firewall port for all FTP sessions across a firewall, which is clearly different from the prevailing FTP protocol which requires two ports (e.g., 20 for data and 21 for control). Furthermore, whatever significance the Sit architecture might have on the system claims 1-11, the indiscriminate application of Sit to the method claims 12-25 would be unjustified. As is well known, an applicant can patent a new use of an old system if that new use is novel and nonobvious.

In view of the foregoing, Appellant respectfully urges the Board to avoid any simplistic or intellectually tardy approach in reviewing this Appeal. Specifically, Appellant requests that the Board make an effort to appreciate the technological intricacies beyond the mere physical resemblance between the Sit system and the claimed system.

C. Independent Claim 12 is Patentable over the Cited References

Claim 12 is a method claim that recites, among other things, "*said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall*" and "*restricting all flow of FTP data passing through said security system through a single port on said firewall.*" As discussed above with respect to claim 1, neither Sit nor Underwood discloses or suggests these features. Nor is there any motivation or suggestion found in the prior art for the combination of Sit and Underwood.

Therefore, the Sit-Underwood combination cannot render claim 12 obvious.

D. Dependent Claims 2-11 and 13-25 Are Each Separately Patentable Over the Cited References

Claims 2-11 and 13-25 all depend ultimately from one of independent claims 1 and 12. As such, each of these dependent claims contain each of the elements recited in the independent claims. For the reasons stated above, the cited references fail to disclose or suggest all the elements recited in claims 1 and 12. Thus, for at least the same reasons, the cited references cannot render claims 2-11 or 13-25 obvious. Additionally, claims 2-11 and 13-25 are each separately patentable over the cited references for the additional features that each of these dependent claims recites.

1. Claims 2-10 and 13-24

For example, claims 2-10 and 13-24 are each separately patentable because the cited references fail to disclose the specific procedures for establishing FTP connections and forwarding FTP data as recited in these claims. In addition, there is no teaching or motivation to modify Sit to include these communication procedures.

2. Claims 11 and 25

Claims 11 and 25 are each separately patentable because the cited references fail to disclose all FTP data among multiple servers and client systems being "transferred through said single port on said firewall." Neither Sit nor the other cited references teach or suggest multiplexing all HTTP traffic among multiple server-client pairs through a single port on a firewall. In addition, the Sit system is HTTP-specific and cannot be readily adapted for FTP purposes absent any motivation or suggestion for its modification.

VIII. CLAIMS APPENDIX

Appendix A contains a listing of currently pending claims.

IX. EVIDENCE APPENDIX

No Evidence Appendix is included herewith.

X. RELATED PROCEEDINGS APPENDIX

No Related Proceedings Appendix is included herewith.

XI. CONCLUSION

For the foregoing reasons, Appellant respectfully submits that the cited references fail to render claims 1-25 obvious under 35 U.S.C. §103(a). Accordingly, Appellant respectfully requests reversal of the final rejection of claims 1-25.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

HUNTON & WILLIAMS, LLP

By: 

Ce Li
Registration No. L0214

Hunton & Williams, LLP
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
Telephone (202) 955-1500
Facsimile (202) 778-2201

Dated: December 28, 2006

APPENDIX A: LISTING OF CLAIMS

1. (Original) A system providing secure transfer of data, said system comprising:

a client system;

a server;

a security system interposed between said client system and said server for controlling communications between said client system and said server, said security system including:

a first proxy system and a second proxy system, said first proxy system coupled between said client system and said second proxy system, and said second proxy system coupled between said server and said first proxy system;

a firewall coupled between said first proxy system and said second proxy system, said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall;

wherein all FTP data are transferred between said client system and said server through said single port on said firewall.

2. (Original) The system of claim 1, wherein

said client system provides an identification of said server to said first proxy system;

said first proxy system forwards said identification to said second proxy system through said single port on said firewall; and

said second proxy system uses said identification to establish a data transfer session with said server.

3. (Original) The system of claim 2, wherein said server establishes a command channel with said client system through said security system.

4. (Original) The system of claim 2, wherein said server transmits a representation of a socket to be used for a data channel to said client system.

5. (Original) The system of claim 4, wherein prior to forwarding said represented socket to said client system, said first proxy system modifies said representation of said socket by substituting said first proxy system's IP address for said server's IP address.

6. (Original) The system of claim 5, wherein said client system transmits a request through said security system for data located on said server.

7. (Original) The system of claim 6, wherein said first proxy system forwards said modified request through said single port on said firewall to said server.

8. (Original) The system of claim 7, wherein said second proxy system modifies said request by substituting said server's IP address for said first proxy system's IP address.

9. (Original) The system of claim 8, wherein said server transmits data corresponding to said request to said second proxy system, and said data corresponding to said request for data is forwarded by said second proxy system through said single port on said firewall to said first proxy system.

10. (Original) The system of claim 9, wherein said first proxy system forwards said data

corresponding to said request for data to said client system.

11. (Original) The system of claim 1, further comprising a plurality of servers and a plurality of client systems, wherein all data transferred between said plurality of servers and said plurality of clients are transferred through said single port on said firewall.

12. (Original) A method for providing secure transfer of data, said method comprising:

using a client system to request data;

using a server to provide data;

controlling communications between said client system and said server using a security system, said security system including:

a first proxy system and a second proxy system, said first proxy system coupled between said client system and said second proxy system, and said second proxy system coupled between said server and said first proxy system;

a firewall coupled between said first proxy system and said second proxy system, said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall;

using said security system to transfer said data between said client and said server; and

restricting all flow of FTP data passing through said security system through a single port on said firewall.

13. (Original) The method of claim 12, further comprising

providing to said first proxy system an identification of said server by said client system;

forwarding said identification to said second proxy system by said first proxy system through said single port on said firewall; and

using said identification by said second proxy system to establish a data transfer session with said server.

14. (Original) The method of claim 13, further comprising establishing a command channel by said server with said client system through said security system.

15. (Original) The method of claim 13, further comprising transmitting a representation of a socket to be used for a data channel by said server to said client system.

16. (Original) The method of claim 15, further comprising modifying said representation of said socket by said first proxy system.

17. (Original) The method of claim 16, wherein said modifying step further comprises substituting said first proxy system's IP address for said server's IP address.

18. (Original) The method of claim 17, further comprising forwarding said modified represented socket to said client system.

19. (Original) The method of claim 18, further comprising transmitting a request through said security system for data located on said server by said client system.

20. (Original) The method of claim 19, further comprising modifying said request by said first proxy system, prior to forwarding said request.

21. (Original) The method of claim 20, wherein said modifying step further comprises substituting said server's IP address for said first proxy system's IP address.

22. (Original) The method of claim 21, further comprising forwarding said modified request through said single port on said firewall by said first proxy system to said server.

23. (Original) The method of claim 22, further comprising transmitting data corresponding to said request to said second proxy system by said server, and forwarding said data corresponding to said request by said second proxy system through said single port on said firewall to said first proxy system.

24. (Original) The method of claim 22, further comprising forwarding said data corresponding to said request by said first proxy system to said client system.

25. (Original) The method of claim 12, further comprising requesting data on a plurality of servers by a plurality of client systems.